- Public Law 104-106, Clinger-Cohen Act of 1996 [formerly, Information Technology Management Reform Act (ITMRA)], February 10, 1996.
- Privacy Act of 1974, As Amended. 5 United States Code (U.S.C.) 552a, Public Law 93-579, Washington, D.C., July 14, 1987.
- Executive Order 12829, *National Industrial Security Program*, January 6, 1993.
- Executive Order 12958, *Classified National Security Information*, as amended.
- Executive Order 12968, *Access to Classified Information*, August 2, 1995.
- Executive Order 13231, *Critical Infrastructure Protection in the Information Age*, October 16, 2001.• National Industrial Security Program Operating Manual (NISPOM), February 2001.
- DHS *Sensitive Systems Policy Publication 4300A* v2.1, July 26, 2004
- DHS *National Security Systems Policy Publication 4300B* v2.1, July 26, 2004
- Homeland Security Presidential Directive 7, *Critical Infrastructure Identification, Prioritization, and Protection*, December 17, 2003.
- Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*.
- National Security Directive (NSD) 42, *National Policy for the Security of National Security Telecommunications and Information Systems* (U), July 5, 1990, CONFIDENTIAL.
- 5 Code of Federal Regulations (CFR) §2635, Office of Government Ethics, *Standards of Ethical Conduct for Employees of the Executive Branch.*
- DHS SCG OS-002 (IT), National Security IT Systems Certification & Accreditation, March 2004.
- Department of State 12 Foreign Affairs Manual (FAM) 600, *Information Security Technology*, June 22, 2000.
- Department of State 12 FAM 500, *Information Security*, October 1, 1999.
- Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*, dated April 3, 1984.
- Presidential Decision Directive 67, *Enduring Constitutional Government and Continuity of Government Operations*, dated October 21, 1998.
- FEMA Federal Preparedness Circular 65, *Federal Executive Branch Continuity of Operations (COOP)*, dated July 26, 1999.
- FEMA Federal Preparedness Circular 66, *Test, Training and Exercise (TT&E) for Continuity of Operations (COOP)*, dated April 30, 2001.
- FEMA Federal Preparedness Circular 67, *Acquisition of Alternate Facilities for Continuity of Operations*, dated April 30, 2001.
- Title 36 Code of Federal Regulations 1236, Management of Vital Records, revised as of July 1, 2000.
- National Institute of Standards and Technology (NIST) Special Publications for computer security and FISMA compliance.

GENERAL

Due to the sensitive nature of USCIS information, the contractor is required to develop and maintain a comprehensive Computer and Telecommunications Security Program to address the integrity, confidentiality, and availability of sensitive but unclassified (SBU) information during collection, storage, transmission, and disposal. The contractor's security program shall adhere to

the requirements set forth in the DHS Management Directive 4300 IT Systems Security Pub Volume 1 Part A and DHS Management Directive 4300 IT Systems Security Pub Volume I Part B. This shall include conformance with the DHS Sensitive Systems Handbook, DHS Management Directive 11042 Safeguarding Sensitive but Unclassified (For Official Use Only) Information and other DHS or USCIS guidelines and directives regarding information security requirements. The contractor shall establish a working relationship with the USCIS IT Security Office, headed by the Information Systems Security Program Manager (ISSM).

IT SYSTEMS SECURITY

In accordance with DHS Management Directive 4300.1 "Information Technology Systems Security", USCIS Contractors shall ensure that all employees with access to USCIS IT Systems are in compliance with the requirement of this Management Directive. Specifically, all contractor employees with access to USCIS IT Systems meet the requirement for successfully completing the annual "Computer Security Awareness Training (CSAT)." All contractor employees are required to complete the training within 60-days from the date of entry on duty (EOD) and are required to complete the training yearly thereafter.

CSAT can be accessed at the following: http://otcd.uscis.dhs.gov/EDvantage.Default.asp or via remote access from a CD which can be obtained by contacting uscisitsecurity@dhs.gov.

All services provided under this delivery order must be compliant with DHS Information Security Policy, identified in MD4300.1, Information Technology Systems Security Program and 4300A Sensitive Systems Handbook.

SECURITY REVIEW

The Government may elect to conduct periodic reviews to ensure that the security requirements contained in this contract are being implemented and enforced. The Contractor shall afford DHS including the organization of the DHS Office of the Chief Information Officer, the Office of the Inspector General, authorized Contracting Officer's Technical Representative (COTR), and other government oversight organizations, access to the Contractor's facilities, installations, operations, documentation, databases, and personnel used in the performance of this contract. The Contractor will contact the DHS Chief Information Security Officer to coordinate and participate in the review and inspection activity of government oversight organizations external to the DHS. Access shall be provided to the extent necessary for the government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability, and confidentiality of DHS data or the function of computer systems operated on behalf of DHS, and to preserve evidence of computer crime.

IT SECURITY IN THE SYSTEMS DEVELOPMENT LIFE CYCLE (SDLC)

The USCIS SDLC Manual documents all system activities required for the development, operation, and disposition of IT security systems. Required systems analysis, deliverables, and security activities are identified in the SDLC manual by lifecycle phase. The contractor shall assist the appropriate USCIS ISSO with development and completion of all SDLC activities and deliverables contained in the SDLC. The SDLC is supplemented with information from DHS and USCIS Policies and procedures as well as the National Institute of Standards Special

Procedures related to computer security and FISMA compliance. These activities include development of the following documents:

- *Sensitive System Security Plan (SSSP)*: This is the primary reference that describes system sensitivity, criticality, security controls, policies, and procedures. The SSSP shall be based upon the completion of the DHS FIPS 199 workbook to categorize the system of application and completion of the RMS Questionnaire. The SSSP shall be completed as part of the System or Release Definition Process in the SDLC and shall not be waived or tailored.
- *Privacy Impact Assessment (PIA) and System of Records Notification (SORN).* For each new development activity, each incremental system update, or system recertification, a PIA and SORN shall be evaluated. If the system (or modification) triggers a PIA the contractor shall support the development of PIA and SORN as required. The Privacy Act of 1974 requires the PIA and shall be part of the SDLC process performed at either System or Release Definition.
- *Contingency Plan (CP)*: This plan describes the steps to be taken to ensure that an automated system or facility can be recovered from service disruptions in the event of emergencies and/or disasters. The Contractor shall support annual contingency plan testing and shall provide a Contingency Plan Test Results Report.
- *Security Test and Evaluation (ST&E)*: This document evaluates each security control and countermeasure to verify operation in the manner intended. Test parameters are established based on results of the RA. An ST&E shall be conducted for each Major Application and each General Support System as part of the certification process. The Contractor shall support this process.
- *Risk Assessment (RA):* This document identifies threats and vulnerabilities, assesses the impacts of the threats, evaluates in-place countermeasures, and identifies additional countermeasures necessary to ensure an acceptable level of security. The RA shall be completed after completing the NIST 800-53 evaluation, Contingency Plan Testing, and the ST&E. Identified weakness shall be documented in a Plan of Action and Milestone (POA&M) in the USCIS Trusted Agent FISMA (TAF) tool. Each POA&M entry shall identify the cost of mitigating the weakness and the schedule for mitigating the weakness, as well as a POC for the mitigation efforts.
- *Certification and Accreditation (C&A):* This program establishes the extent to which a particular design and implementation of an automated system and the facilities housing that system meet a specified set of security requirements, based on the RA of security features and other technical requirements (certification), and the management authorization and approval of a system to process sensitive but unclassified information (accreditation). As appropriate the Contractor shall be granted access to the USCIS TAF and Risk Management System (RMS) tools to support C&A and its annual assessment requirements. Annual assessment activities shall include completion of the NIST 800-26 Self Assessment in TAF, annual review of user accounts, and annual review of the FIPS categorization. C&A status shall be reviewed for each incremental system update and a new full C&A process completed when a major system revision is anticipated.

SECURITY REQUIREMENTS FOR UNCLASSIFIED INFORMATION TECHNOLOGY RESOURCES

(a) The Contractor shall be responsible for Information Technology (IT) security for all systems connected to a DHS network or operated by the Contractor for DHS, regardless of location. This clause applies to all or any part of the contract that includes information technology resources or services for which the Contractor must have physical or electronic access to sensitive information contained in DHS unclassified systems that directly support the agency's mission.

(b) The Contractor shall provide, implement, and maintain an IT Security Plan. This plan shall describe the processes and procedures that will be followed to ensure appropriate security of IT resources that are developed, processed, or used under this contract.

(1) Within 30 days after contract award, the contractor shall submit for approval its IT Security Plan, which shall be consistent with and further detail the approach contained in the offeror's proposal. The plan, as approved by the Contracting Officer, shall be incorporated into the contract as a compliance document.

(2) The Contractor's IT Security Plan shall comply with Federal laws that include, but are not limited to, the Computer Security Act of 1987 (40 U.S.C. 1441 et seq.); the Government Information Security Reform Act of 2000; and the Federal Information Security Management Act of 2002; and with Federal policies and procedures that include, but are not limited to, OMB Circular A-130.

(3) The security plan shall specifically include instructions regarding handling and protecting sensitive information at the Contractor's site (including any information stored, processed, or transmitted using the Contractor's computer systems), and the secure management, operation, maintenance, programming, and system administration of computer systems, networks, and telecommunications systems.

(c) Examples of tasks that require security provisions include--

(1) Acquisition, transmission or analysis of data owned by DHS with significant replacement cost should the contractor's copy be corrupted; and

(2) Access to DHS networks or computers at a level beyond that granted the general public (e.g., such as bypassing a firewall).

(d) At the expiration of the contract, the contractor shall return all sensitive DHS information and IT resources provided to the contractor during the contract, and certify that all non-public DHS information has been purged from any contractor-owned system. Components shall conduct reviews to ensure that the security requirements in the contract are implemented and enforced.

(e) Within 6 months after contract award, the contractor shall submit written proof of IT Security accreditation to DHS for approval by the DHS Contracting Officer. Accreditation will proceed according to the criteria of the DHS Sensitive System Policy Publication, 4300A (Version 5.5, September 30, 2007) or any replacement publication, which the Contracting Officer will provide upon request. This accreditation will include a final security plan, risk

assessment, security test and evaluation, and disaster recovery plan/continuity of operations plan. This accreditation, when accepted by the Contracting Officer, shall be incorporated into the contract as a compliance document. The contractor shall comply with the approved accreditation documentation.

CONTRACTOR EMPLOYEE ACCESS

(a) *Sensitive Information*, as used in this Chapter, means any information, the loss, misuse, disclosure, or unauthorized access to or modification of which could adversely affect the national or homeland security interest, or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:

(1) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Public Law 107-296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, Part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);

(2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, "Policies and Procedures of Safeguarding and Control of SSI," as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee);

(3) Information designated as "For Official Use Only," which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and

(4) Any information that is designated "sensitive" or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security information handling procedures.

(b) "Information Technology Resources" include, but are not limited to, computer equipment, networking equipment, telecommunications equipment, cabling, network drives, computer drives, network software, computer software, software programs, intranet sites, and internet sites.

(c) Contractor employees working on this contract must complete such forms as may be necessary for security or other reasons, including the conduct of background investigations to determine suitability. Completed forms shall be submitted as directed by the Contracting Officer. Upon the Contracting Officer's request, the Contractor's employees shall be fingerprinted, or subject to other investigations as required. All contractor employees requiring recurring access to

Government facilities or access to sensitive information or IT resources are required to have a favorably adjudicated background investigation prior to commencing work on this contract unless this requirement is waived under Departmental procedures.

(d) The Contracting Officer may require the contractor to prohibit individuals from working on the contract if the government deems their initial or continued employment contrary to the public interest for any reason, including, but not limited to, carelessness, and insubordination, incompetence, or security concerns.

(e) Work under this contract may involve access to sensitive information. Therefore, the Contractor shall not disclose, orally or in writing, any sensitive information to any person unless authorized in writing by the Contracting Officer. For those contractor employees authorized access to sensitive information, the contractor shall ensure that these persons receive training concerning the protection and disclosure of sensitive information both during and after contract performance.

(f) The Contractor shall include the substance of this clause in all subcontracts at any tier where the subcontractor may have access to Government facilities, sensitive information, or resources.

(g) Before receiving access to IT resources under this contract the individual must receive a security briefing, which the Contracting Officer's Technical Representative (COTR) will arrange, and complete any nondisclosure agreement furnished by DHS.

(h) The contractor shall have access only to those areas of DHS information technology resources explicitly stated in this contract or approved by the COTR in writing as necessary for performance of the work under this contract. Any attempts by contractor personnel to gain access to any information technology resources not expressly authorized by the statement of work, other terms and conditions in this contract, or as approved in writing by the COTR, is strictly prohibited. In the event of violation of this provision, DHS will take appropriate actions with regard to the contract and the individual(s) involved.

(i) Contractor access to DHS networks from a remote location is a temporary privilege for mutual convenience while the contractor performs business for the DHS Component. It is not a right, a guarantee of access, a condition of the contract, or Government Furnished Equipment (GFE).

(j) Contractor access will be terminated for unauthorized use. The contractor agrees to hold and save DHS harmless from any unauthorized use and agrees not to request additional time or money under the contract for any delays resulting from unauthorized use or access.

(k) Non-U.S. citizens shall not be authorized to access or assist in the development, operation, management or maintenance of Department IT systems under the contract, unless a waiver has been granted by the Head of the Component or designee, with the concurrence of both the Department's Chief Security Officer (CSO) and the Chief Information Officer (CIO) or

their designees. Within DHS Headquarters, the waiver may be granted only with the approval of both the CSO and the CIO or their designees. In order for a waiver to be granted:

(1) The individual must be a legal permanent resident of the U.S. or a citizen of Ireland, Israel, the Republic of the Philippines, or any nation on the Allied Nations List maintained by the Department of State;

(2) There must be a compelling reason for using this individual as opposed to a U.S. citizen; and

(3) The waiver must be in the best interest of the Government.

(l) Contractors shall identify in their proposals the names and citizenship of all non-U.S. citizens proposed to work under the contract. Any additions or deletions of non-U.S. citizens after contract award shall also be reported to the contracting officer.

SECURITY ASSURANCES

DHS Management Directives 4300 requires compliance with standards set forth by NIST, for evaluating computer systems used for processing SBU information. The Contractor shall ensure that requirements are allocated in the functional requirements and system design documents to security requirements are based on the DHS policy, NIST standards and applicable legislation and regulatory requirements. Systems shall offer the following visible security features:

- *User Identification and Authentication (I&A)* – I&A is the process of telling a system the identity of a subject (for example, a user) (*I*) and providing that the subject is who it claims to be (*A*). Systems shall be designed so that the identity of each user shall be established prior to authorizing system access, each system user shall have his/her own user ID and password, and each user is authenticated before access is permitted. All system and database administrative users shall have strong authentication, with passwords that shall conform to established DHS standards. All USCIS Identification and Authentication shall be done using the Password Issuance Control System (PICS) or its successor. Under no circumstances will Identification and Authentication be performed by other than the USCIS standard system in use at the time of a systems development.
- *Discretionary Access Control (DAC)* – DAC is a DHS access policy that restricts access to system objects (for example, files, directories, devices) based on the identity of the users and/or groups to which they belong. All system files shall be protected by a secondary access control measure.
- *Object Reuse* – Object Reuse is the reassignment to a subject (for example, user) of a medium that previously contained an object (for example, file). Systems that use memory to temporarily store user I&A information and any other SBU information shall be cleared before reallocation.
- *Audit* – DHS systems shall provide facilities for transaction auditing, which is the examination of a set of chronological records that provide evidence of system and user activity. Evidence of active review of audit logs shall be provided to the USCIS IT Security Office on a monthly basis, identifying all security findings including failed log in attempts, attempts to access restricted information, and password change activity.

- *Banner Pages* – DHS systems shall provide appropriate security banners at start up identifying the system or application as being a Government asset and subject to government laws and regulations. This requirement does not apply to public facing internet pages, but shall apply to intranet applications.

DATA SECURITY

SBU systems shall be protected from unauthorized access, modification, and denial of service. The Contractor shall ensure that all aspects of data security requirements (i.e., confidentiality, integrity, and availability) are included in the functional requirements and system design, and ensure that they meet the minimum requirements as set forth in the DHS Sensitive Systems Handbook and USCIS policies and procedures. These requirements include:

- *Integrity* – The computer systems used for processing SBU shall have data integrity controls to ensure that data is not modified (intentionally or unintentionally) or repudiated by either the sender or the receiver of the information. A risk analysis and vulnerability assessment shall be performed to determine what type of data integrity controls (e.g., cyclical redundancy checks, message authentication codes, security hash functions, and digital signatures, etc.) shall be used.
- *Confidentiality* – Controls shall be included to ensure that SBU information collected, stored, and transmitted by the system is protected against compromise. A risk analysis and vulnerability assessment shall be performed to determine if threats to the SBU exist. If it exists, data encryption shall be used to mitigate such threats.
- *Availability* – Controls shall be included to ensure that the system is continuously working and all services are fully available within a timeframe commensurate with the availability needs of the user community and the criticality of the information processed.
- *Data Labeling.* – The contractor shall ensure that documents and media are labeled consistent with the DHS *Sensitive Systems Handbook.*

19.0 Homeland Security Enterprise Architecture (HLS EA)Compliance

All solutions and services shall meet DHS Enterprise Architecture policies, standards, and procedures as it relates to this Statement of Work. Specifically, the Contractor shall comply with the following Homeland Security Enterprise Architecture (HLS EA) requirements:

- All developed solutions and requirements shall be compliant with the HLS EA.
- All IT hardware or software shall be compliant with the HLS EA Technology Reference Model (TRM) Standards and Products Profile.
- All data assets, information exchanges and data standards, whether adopted or developed, shall be submitted to the DHS Enterprise Data Management Office (EDMO) for review and insertion into the DHS Data Reference Model.

The Contractor shall provide, the full range of business and technical management services that assist in the development and implementation, of IT products and services that are compliant with the USCIS Enterprise Architecture, as well as the DHS Enterprise Architecture policies, procedures, guidelines, and directives (e.g., EA reference models, Investment Review Process). All IT products and services provided by the Contractor shall be subject to EA governance oversight performed by USCIS Office of Information Technology (OIT).

The contractor shall comply with the following Homeland Security Enterprise Architecture (HLS EA) requirement:

- In compliance with OMB mandates, all network hardware shall be IPv6 compatible without modification, upgrade, or replacement.

20.0 List of Attachments

Attachment A – List of Existing Live-Scan Systems for Disposal and New Equipment for Installation, by USCIS Location

Attachment B – ASC Store and Forward Configurations

Attachment C – Biometrics Capture Flow Chart

Attachment D – Live-Scan Deployment Schedule

Attachment E – UKvisas Software Requirements

Attachment F – FBI Appendix F

Additional Delivery Order Terms and Conditions

52.252-2 Clauses Incorporated by Reference. (FEB 1998)

This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this/these address (es): http://www.acquisition.gov/far

(End of clause)

52.217-9 Option to Extend the Term of the Contract (MAR 2000)

(a) The Government may extend the term of this contract by written notice to the Contractor within 30 days provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 60 days before the contract expires. The preliminary notice does not commit the Government to an extension.

(b) If the Government exercises this option, the extended contract shall be considered to include this option clause.

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed 3 years.

(End of clause)

52.251-1 Government Supply Sources (APR 1984)

The Contracting Officer may issue the Contractor an authorization to use Government supply sources in the performance of this contract. Title to all property acquired by the Contractor under such an authorization shall vest in the Government unless otherwise specified in the contract. Such property shall not be considered to be "Government-furnished property," as distinguished from "Government property." The provisions of the clause entitled "Government Property," except its paragraphs (a) and (b), shall apply to all property acquired under such authorization.

(End of clause)

Homeland Security Acquisition Regulation (HSAR) clauses and provisions incorporated by reference.

FAR clause 52.252-2, this contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of HSAR clauses may be accessed electronically at this internet address:

http://www.dhs.gov/xlibrary/assets/opnbiz/cpo_hsar_finalrule.pdf

3052.242-71 Dissemination of Contract Information (DEC 2003)

3052.242-72 Contracting officer's technical representative (DEC 2003)

Homeland Security Acquisition Regulation Clauses & Provisions in Full Text

3052.204-71, Contractor Employee Access (JUN 2006)

(a) *Sensitive Information,* as used in this Chapter, means any information, the loss, misuse, disclosure, or unauthorized access to or modification of which could adversely affect the national or homeland security interest, or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:

(1) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Public Law 107-296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, Part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);

(2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, "Policies and Procedures of Safeguarding and Control of S SI," as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee);

(3) Information designated as "For Official Use Only," which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and

(4) Any information that is designated "sensitive" or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security information handling procedures.

(b) "Information Technology Resources" include, but are not limited to, computer equipment, networking equipment, telecommunications equipment, cabling, network drives, computer drives, network software, computer software, software programs, intranet sites, and internet sites.

(c) Contractor employees working on this contract must complete such forms as may be necessary for security or other reasons, including the conduct of background investigations to determine suitability. Completed forms shall be submitted as directed by the Contracting Officer. Upon the Contracting Officer's request, the Contractor's employees shall be fingerprinted, or subject to other investigations as required. All contractor employees requiring recurring access to Government facilities or access to sensitive information or IT resources are required to have a

favorably adjudicated background investigation prior to commencing work on this contract unless this requirement is waived under Departmental procedures.

(d) The Contracting Officer may require the contractor to prohibit individuals from working on the contract if the government deems their initial or continued employment contrary to the public interest for any reason, including, but not limited to, carelessness, and insubordination, incompetence, or security concerns.

(e) Work under this contract may involve access to sensitive information. Therefore, the Contractor shall not disclose, orally or in writing, any sensitive information to any person unless authorized in writing by the Contracting Officer. For those contractor employees authorized access to sensitive information, the contractor shall ensure that these persons receive training concerning the protection and disclosure of sensitive information both during and after contract performance.

(f) The Contractor shall include the substance of this clause in all subcontracts at any tier where the subcontractor may have access to Government facilities, sensitive information, or resources.

(End of clause)

Performance Reporting

For active contracts valued in excess of simplified acquisition threshold, the Federal Acquisition Regulation (FAR) 42.1502 requires federal agencies to prepare Contractor performance evaluations. Performance evaluations are completed and forwarded to the Contractor for review within thirty (30) calendar days from the time the work under the contract is completed for each contract year. Interim evaluations by the Contracting Officer may be completed as necessary. The Contractor has thirty (30) days to reply with comments, rebutting statements, or additional information that will be made part of the official record.

Invoicing Requirements

The Statement of Work contains the invoicing requirement instructions. The invoice shall be sent via e-mail to the USCIS COTR and the USCIS Contracting Officer. The payment office address is as follows:

Dallas Finance Center
PO Box 561547
Dallas, TX 75356-1547

Advertisements, Publicizing Awards & News Releases

All Press releases or announcements about agency programs, projects, and contract awards need to be cleared by the Program Office and the Contracting Officer. Under no circumstances shall the Contractor, or anyone acting on behalf of the Contractor, refer to the supplies, services, or equipment furnished pursuant to the provisions of this contract in any publicity news release or

commercial advertising without first obtaining explicit written consent to do so from the Program Office and the Contracting officer.

The Contractor agrees not to refer to awards in commercial advertising in such a manner as to state or imply that the product or service provided is endorsed or preferred by the Federal Government or is considered by the Government to be superior to other products or services.

Organizational Conflict of Interest

(a) The Contractor warrants that, to the best of the Contractor's knowledge and belief, there are no relevant facts or circumstances which could give rise to an organizational conflict of interest, as defined in FAR Subpart 9.5, or that the Contractor has disclosed all such relevant information.

(b) Prior to commencement of any work, the Contractor agrees to notify the CO immediately that to the best of its knowledge and belief, no actual or potential conflict of interest exists or to identify to the CO any actual or potential conflict of interest the firm may have. In emergency situations, however, work may begin but notification shall be made within five (5) working days.

(c) The Contractor agrees that if an actual or potential organizational conflict of interest is identified during performance, the Contractor shall immediately make a full disclosure in writing to the CO. This disclosure shall include a description of actions which the Contractor has taken or proposes to take, after consultation with the CO, to avoid, mitigate, or neutralize the actual or potential conflict of interest. The Contractor shall continue performance until notified by the CO of any contrary action to be taken.

(d) Remedies – USCIS may terminate this contract for convenience, in whole or in part, if it deems such termination necessary to avoid organizational conflict of interest. If the Contractor was aware of a potential organizational conflict of interest prior to award or discovered an actual or potential conflict after award and did not disclose it or misrepresented relevant information to the CO, the Government may terminate the contract for default, debar the Contractor from Government contracting, or pursue such other remedies as may be permitted by law or this contract.

Contractor Employee Suitability Determinations

In accordance with the Security Requirements contained the Statement of Work, employees requiring USCIS Information System access for installation of images or system configuration require Suitability Determinations. The Security Requirement section of the SOW details the requirements of the Suitability Determinations. **To expedite processing of appropriate suitability documentation, contractor is required to submit documentation within 10 calendar days of award.**

HSSCCG-10-J-00034 ATTACHMENT A - List of USCIS Locations with Current Live-Scan Systems for Disposal and New Live-Scan Systems for Installation

Type	Site Name	Site Code	Street	City	State	Zipcode	Disposal			Installation		
							Cabinet	Desktop	Mobile	Cabinet	Desktop	Mobile
NORTHEAST REGION												
DISTRICT 1												
SA	Boston	XBD	170 Portland St	Boston	MA	02114-1706	9			7		1
SA	Providence	XBF	105 Sockanosset Cross Rd, Suite 210	Cranston	RI	02920-5560	4			3		1
COLO	Manchester	XBG	803 Canal St	Manchester	NH	03101-1226	2			2		
COLO	Portland, ME	XPJ	176 Gannett Drive	South Portland	ME	04106-6909	1			2		
COLO	Lawrence	XBK	2 Mill Street	Lawrence	MA	01840-1602	2			2	1	
DISTRICT 2												
COLO	Buffalo	XBH	130 Delaware Ave	Buffalo	NY	14202-2498	2			2		1
COLO	Albany	XBI	1086 Troy-Schenectady Hwy	Latham	NY	12110-1024	2			2		
COLO	St. Albans, VT	XPK	64 Gricebrook Rd	St. Albans	VT	05478-9500	1			1	1	
SA	Hartford	XBE	467 Silver Lane	East Hartford	CT	06118-1104	4			3		1
COLO	Syracuse	XBJ	412 S. Warren St	Syracuse	NY	13202-2604	2			2		
DISTRICT 3												
SA	New Rochelle	XNG	246 North Ave	New Rochelle	NY	10801-6405	7			4	1	1
SA	Brooklyn	XNI	1260-1278 60th St	Brooklyn	NY	11219-4929	15			9	1	1
SA	Bronx	XNJ	1827 Westchester Ave	Bronx	NY	10472-3017	9			5	1	1
COLO	Manhattan	XNK	201 W Houston St. Street Entrance send mail & DHL to 201 Varick St, Suite 1023	New York	NY	10014-4811	11			7	1	
SA	Hicksville (Hempstead)	XNL	87 Bethpage Road	Hicksville	NY	11801-1503	6			4		1
SA	Queens/ Jamaica	XNM	153-01 Jamaica Ave	Jamaica	NY	11432-4910	10			5	2	
SA	Woodside	XNN	63-05 Roosevelt Ave	Woodside	NY	11377-3641	9			6	1	1
DISTRICT 4												
SA	Elizabeth	XNO	285 North Broad St	Elizabeth	NJ	07208-2303	18			11	1	1
SA	Hackensack	XNP	116 Kansas Street, Main Floor	Hackensack	NJ	07601-7103	4			3		1
DISTRICT 5												
SA	Philadelphia	XPA	10300 Drummond Rd, Suite 100	Philadelphia	PA	19154-3804	9	1		6	1	1
SA	Pittsburgh	XPB	800 Penn Ave, Suite 101	Pittsburgh	PA	15222-3615	2			2		1
COLO	Charleston, WV	XPC	210 Kanawha Blvd West	Charleston	WV	25302-2201	1			1	1	
SA	Dover	XPD	250 Gateway South Blvd, Suites: 260 & 270	Dover	DE	19901-4699	2	1		1	1	1
COLO	York	XPE	3400 Concord Rd, Old Farm House	York	PA	17402-9007	2			2		
DISTRICT 6												
SA	Baltimore	XBA	100 South Charles St, Suite 201	Baltimore	MD	21201-2701	6			4	1	1
SA	Glenmont	XBB	12331 Georgia Ave, Glenmont Plaza, Suite C	Wheaton	MD	20906-3646	7			4	1	1
SA	Salisbury	XBC	2040 Shipley Drive Suite C2	Salisbury	MD	21801-7874	1			1	1	1
DISTRICT 7												
SA	Alexandria	XDE	8850 Richmond Hwy, Suite 100	Alexandria	VA	22309-1586	11	1		6	1	1
SA	Norfolk	XDF	2500 Almeda Ave, Suite 114	Norfolk	VA	23513-2503	1	1		2		1

Type	Site Name	Site Code	Street	City	State	Zipcode	Cabinet	Desktop	Mobile	Cabinet	Desktop	Mobile
SOUTHEAST REGION												
DISTRICT 9												
SA	Atlanta	XAC	1255 Collier Road, Suite 100	Atlanta	GA	30318-2308	10	1		7	2	1
SA	Birmingham	XAB	529 Beacon Parkway, Suite 106	Birmingham	AL	35209-3126	2			2	1	1
SA	Charlotte	XAD	4801 Chastain Ave, Building 10, Suite 175	Charlotte	NC	28217-2231	5			3	1	1
COLO	Charleston, SC	XAE	1 Poston Rd, Suite 130 Parkshore Center	Charleston	SC	29407-3424	1	1		2		1
COLO	Raleigh	XAF	301 Roycroft Drive	Durham	NC	27703-8226	2	1		3	1	1
DISTRICT 8												
COLO	Hialeah	XMA	5880 NW 183rd St	Hialeah	FL	33015-6023	11			7	1	
COLO	Miami	XMB	8801 NW 7th Ave	Miami	FL	33150-2303	8			6	1	1
				Miami	FL	33186	7			5	1	
COLO	Kendall	XMC	14675 SW 120th St	Oakland Park	FL	33309	8			5	1	
COLO	Oakland Park	XMD	4451 NW 31st Ave	Guaynabo	PR	00968-	3			2	1	1
ASC	San Juan	XPM	Metro Office Park TLD Building, 2nd Street, Suite 200	S St. Thomas	VI	00802-5838	1			1	1	
COLO	St. Thomas	XPO	8000 Nisky Center, Suite 1A, Lower Level South, 1st Floor	St. Croix USVI	VI	00821-1468	1			1	1	
COLO	St. Croix	XPP	5-8A Sunny Isle Shopping Center, Christiansted									
DISTRICT 10												
SA	Tampa	XMF	9325 Bay Plaza Blvd, Suite 215	Tampa	FL	33619-4463	6			4	1	1
SA	Orlando	XME	5449 S. Semoran Blvd, #18C	Orlando	FL	32822-1778	5	1		4	1	1
COLO	Jacksonville	XMG	4121 Southpoint Blvd.	Jacksonville	FL	32216-0930	2	2		3		
COLO	West Palm Beach	XMH	2711 Exchange Ct	W Palm Beach	FL	33409-4017	5	1		4	1	1
SA	Fort Myers	XMJ	3850 Colonial Blvd, Suite 100	Fort Myers	FL	33966	2			2	1	1
DISTRICT 11												
COLO	New Orleans	XNA	2424 Edenborn Ave, Suite 300	Metairie	LA	70001-1845	0	2		2	1	1
COLO	Ft. Smith	XNB	4977 Old Greenwood Rd	Ft. Smith	AR	72903-6906	1			1	1	
COLO	Jackson, MS	XNC	100 W. Capitol St, Suite 727	Jackson	MS	39269-1602	1			1	1	
COLO	Memphis	XND	842 Virginia Run Cove	Memphis	TN	38122-4419	2	1		2	1	1
SA	Nashville	XNE	1400 Donelson Pike, Suite B-13	Nashville	TN	37217-0000	2	1		2	1	1
CENTRAL REGION												
DISTRICT 12												
COLO	Detroit	XDK	11411 East Jefferson Ave	Detroit	MI	48214-3332	4	2		4	1	1
SA	Grand Rapids	XDM	4484 Breton Rd	Kentwood	MI	49508-5270	4			2	1	1
DISTRICT 13												
COLO	Cleveland	XCI	1240 E 9th St, Room 1259	Cleveland	OH	44199-2085	3			2		1
COLO	Cincinnati	XCJ	550 Main St, Room 1524	Cincinnati	OH	45202-5298	2	1		2		1
SA	Columbus	XCK	50 W. Broad St, Suite 650	Columbus	OH	43215-5903	3			2		1
COLO	Louisville	XNF	601 W. Broadway, Room 22	Louisville	KY	40202-2250	2	1		2		
COLO	Indianapolis	XCG	950 N. Meridian St, Room 400	Indianapolis	IN	46204-3915	2					

Type	Site Name	Site Code	Street	City	State	Zipcode	Cabinet	Desktop	Mobile	Cabinet	Desktop	Mobile
DISTRICT 14												
SA	Norridge	XCA	4701 N. Cumberland, 1-3 BCD	Norridge	IL	60706-2905	5			3	1	1
SA	Pulaski	XCB	5180 S. Pulaski Rd, Suite 101	Chicago	IL	60632-4253	5	1		3	1	1
SA	Broadway	XCC	4853 N. Broadway	Chicago	IL	60640-3603	5	1		3	1	1
SA	Naperville	XCD	888 South Route 59, Suite 124	Naperville	IL	60540-0962	5			3	1	1
SA	Waukegan	XCE	25 S. Greenbay Rd	Waukegan	IL	60085-4815	4			2	1	1
SA	Michigan City	XCF	284 Dunes Plaza	Michigan City	IN	46360-7340	3			2	1	
COLO	Milwaukee	XCH	310 E. Knapp St, Room 154	Milwaukee	WI	53202-4504	3	1		3		
DISTRICT 15												
COLO	Kansas City	XKA	9747 N. Conent Ave	Kansas City	MO	64153-1833	2	1		2	1	1
COLO	Wichita	XKB	271 W. 3rd St. North, Suite 1050	Wichita	KS	67202-1212	1			1	1	
COLO	St. Louis	XKC	1222 Spruce St, Room 1.208	St. Louis	MO	63103-2815	2	2		2	1	1
COLO	Omaha	XOA	1717 Avenue H	Omaha	NE	68110-2752	2			2		
COLO	Des Moines	XOB	210 Walnut St, Room 949	Des Moines	IA	50309-2110	2			2		1
SA	St. Paul	XSI	1360 University Ave	St. Paul	MN	55104-4086	4			3	1	1
SA	Rapid City	XSJ	2255 Haines Ave, Suite 214	Rapid City	SD	57701-0411	1			1	1	
COLO	Fargo	XSK	657 2nd Ave. North, Room #248	Fargo	ND	58102-4727	1			1	1	
COLO	Sioux Falls	XSL	300 E. 8th St	Sioux Falls	SD	57103-7023	1			1	1	
COLO	Duluth	XSM	515 W. First St, Suite 208	Duluth	MN	55802-1301	1					
DISTRICT 16												
SA	Dallas North	XDA	10051 Whitehurst Dr, Suite 200	Dallas	TX	75243-0637	5	1		4	1	1
SA	Ft. Worth	XDB	4200 S. Freeway, Suite 1309	Ft. Worth	TX	76115-1400	3	2		3	1	1
SA	Lubbock	XDC	3502 Slide Rd, Suite A-24	Lubbock	TX	79414-2547	2			2		1
COLO	Oklahoma	XDD	4400 S.W. 44th St, Suite A	Oklahoma City	OK	73119-2800	1	1		2		1
SA	Dallas South	XDL	7334 South Westmoreland Rd	Dallas	TX	75237-2908	3			2	1	1
DISTRICT 17												
SA	Houston SE	XHH	8505 Gulf Freeway, Suite A	Houston	TX	77017-5043	5			3	2	1
SA	Houston SW	XHI	11777 State Hwy 6 South	Sugar Land	TX	77498-5721	5	1		4	1	1
SA	Houston NW	XHJ	10555 Northwest Freeway, Suite 150	Houston	TX	77092-8209	4	1		4		1
DISTRICT 18												
SA	San Antonio	XSA	5121 Crestway, Suite 112	San Antonio	TX	78239-1975	4	1		3	1	1
SA	Austin	XSN	Parkline Plaza Shopping Center 11301 Lakeline Blvd, Suite 150	Austin	TX	78717	2			2	1	1
SA	Laredo	XJX	707 E. Calton Rd, Suite 301	Laredo	TX	78041-3638	2			3		1
SA	El Paso	XEA	10500 Montwood	El Paso	TX	79935-2703	4			3		1
SA	Albuquerque	XEC	1605 Isleta Blvd SW, Suite C	Albuquerque	NM	87105-4793	2			2		1
SA	McAllen	XHA	220 South Bicentennial, Suite C	McAllen	TX	78501-7051	3			2	1	1
COLO	Harlingen	XHB	1717 Zoy St	Harlingen	TX	78552-3220	2			2		

Type	Site Name	Site Code	Street	City	State	Zipcode	Cabinet	Desktop	Mobile	Cabinet	Desktop	Mobile
DISTRICT 10												
SA	Denver	XDG	15037 E. Colfax Ave, Unit G	Aurora	CO	80011-6777	5			4	1	1
SA	Grand Junction	XDH	2454 Hwy 6 and 50, Valley Plaza, Suite 115	Grand Junction	CO	81505-1111	1			1	1	1
COLO	Casper	XDI	150 East B St, Room 1014	Casper	WY	82601-7005	1			1	1	
SA	Salt Lake City	XDJ	5536 S, 1900 West St, Bldg C	Taylorsville	UT	84118-9007	3			2	1	1
COLO	Helena	XHC	2800 Skyway Dr	Helena	MT	59602-1230	1			1	1	
COLO	Boise	XHD	1185 South Vinnell Way	Boise	ID	83709-1656	1			1	1	
SA	Idaho Falls	XHE	2265 W. Broadway, Suite A	Idaho Falls	ID	83402-2996	1			1	1	1
WESTERN REGION												
DISTRICT 20												
COLO	Seattle	XSE	12500 Tukwila International Blvd	Seattle	WA	98168-2506	6	1		4	2	1
COLO	Spokane	XSF	920 West Riverside, Room 691	Spokane	WA	99201-1090	1			1	1	
COLO	Yakima	XSH	415 N. 3rd St	Yakima	WA	98901-2331	1	1		2		
COLO	Anchorage	XAA	620 E. 10th Ave, Suite 108	Anchorage	AK	99501-3799	1			1	1	1
SA	Portland, OR	XPL	721 SW 14th Ave	Portland	OR	97205-1840	4	1		3	1	1
DISTRICT 21												
SA	San Francisco	XTD	250 Broadway	San Francisco	CA	94111-1506	9			5	1	1
SA	Oakland	XFB	2040 Telegraph Ave	Oakland	CA	94612-2306	9	1		6	1	1
SA	Santa Rosa	XFC	1401 Guerneville Rd, Room 100	Santa Rosa	CA	95403-4174	3			2		1
SA	Salinas	XFD	1954 N. Main St	Salinas	CA	93906-2305	2			2		1
SA	San Jose	XTE	122 Charcot Ave	San Jose	CA	95131-1101	7			5	1	1
DISTRICT 22												
SA	Sacramento	XFE	825 Riverside Pkwy, Suite 100	West Sacramento	CA	95605-1502	6	1		4	1	1
SA	Modesto	XFF	901 N. Carpenter Rd, Suite 14	Modesto	CA	95351-1199	4			2	1	1
SA	Fresno	XFG	4893 E. Kings Canyon	Fresno	CA	93727-3811	6			3	1	1
SA	Bakersfield	XFI	4701 Planz Rd, Suite A12	Bakersfield	CA	93309-6349	2	1		2	1	1
DISTRICT 23												
SA	Pomona	XLB	435 W. Mission Blvd, Suite 110	Pomona	CA	91766-1601	3			2	1	1
SA	El Monte	XLC	9251 Garvey Ave, Suite Q	S. El Monte	CA	91733-4611	11			7		1
SA	Gardena	XLD	15715 Crenshaw Blvd, Room B-112	Gardena	CA	90249-4529	7			4	1	1
SA	Van Nuys	XLE	14515 Hamlin St, Suite 200	Van Nuys	CA	91411-1608	11			7	1	1
SA	Bellflower	XLF	17610 Bellflower Blvd, Suite A110	Bellflower	CA	90706-8002	5			3	1	1
SA	Fairfax	XLG	5949 West Pico Blvd	Fairfax	CA	90035-2653	4			4		1
SA	Santa Ana	XLH	1666 N. Main St, Suite 100A	Santa Ana	CA	92701-7417	8			4	1	1
SA	Buena Park	XLI	8381 La Palma Ave, Suite A	Buena Park	CA	90620-3207	6			3	1	1
SA	Riverside	XLJ	10082 Magnolia Ave	Riverside	CA	92503-3530	9			5	1	1
SA	Oxnard	XLK	2000 Outlet Center Drive, Suite 200	Oxnard	CA	93036-0609	4			3	1	1
SA	Goleta	XLL	6831-B Hollister Ave	Goleta	CA	93117-3015	3			0		
SA	Wilshire	XLM	1015 Wilshire Blvd	Los Angeles	CA	90017-2602	9			5	1	1

Type	Site Name	Site Code	Street	City	State	Zipcode	Cabinet	Desktop	Mobile	Cabinet	Desktop	Mobile
DISTRICT 24										4	1	1
SA	San Diego	XSB	1261 Third Ave, Suite H	Chula Vista	CA	91911-3262	5	2		3		1
SA	San Marcos	XSC	727 W. San Marcos Blvd, Suite 101-103	San Marcos	CA	92078-1244	4			2		
COLO	Imperial	XSD	509 Industry Way	Imperial	CA	92251-7503	2					
DISTRICT 25										5	2	1
SA	Phoenix	XPQ	2545 E. Thomas Rd	Phoenix	AZ	85016-7941	8	1		4		1
SA	Las Vegas	XPF	6175 S. Pecos Rd	Las Vegas	NV	89120-6284	2	2		2		1
SA	Tucson	XPG	1835 S. Alvernon, Suite 218	Tucson	AZ	85711-5693	3			2		
COLO	Reno	XPH	1351 Corporate Blvd	Reno	NV	89502-7146	1	1		1	1	1
SA	Yuma	XPI	3250 S. 4th Avenue, Suite E	Yuma	AZ	85365-4051	1					
DISTRICT 26										2	1	1
SA	Honolulu	XHF	677 Ala Moana Blvd, Suite 102 & 103	Honolulu	HI	96813-4999	3	1		1	1	
COLO	Agana	XHG	Sirena Plaza, 108 Hernan Cortez Ave, Suite 100	Hagatna	GU	96910-5009	1			1	1	1
SA	Saipan	XHS	TSL Plaza Building, Beach Rd South	Garapan	MP	MP-96950	1					
							544	45		399	98	98
USCIS	ASC Lab	HQ					1		12	1	1	1
USCIS	Image Lab	HQ								0	1	1
						Current Total	545	45	12	400	100	100
						Total Available				400	100	100
	Number of Sites =	134										

ASC STORE AND FORWARD CONFIGURATIONS

ASC Software:

Microsoft Windows 2003 Server
Microsoft SMTP
POP3
Query and Report software not required; use Crystal Reports executables

ASC Hardware:

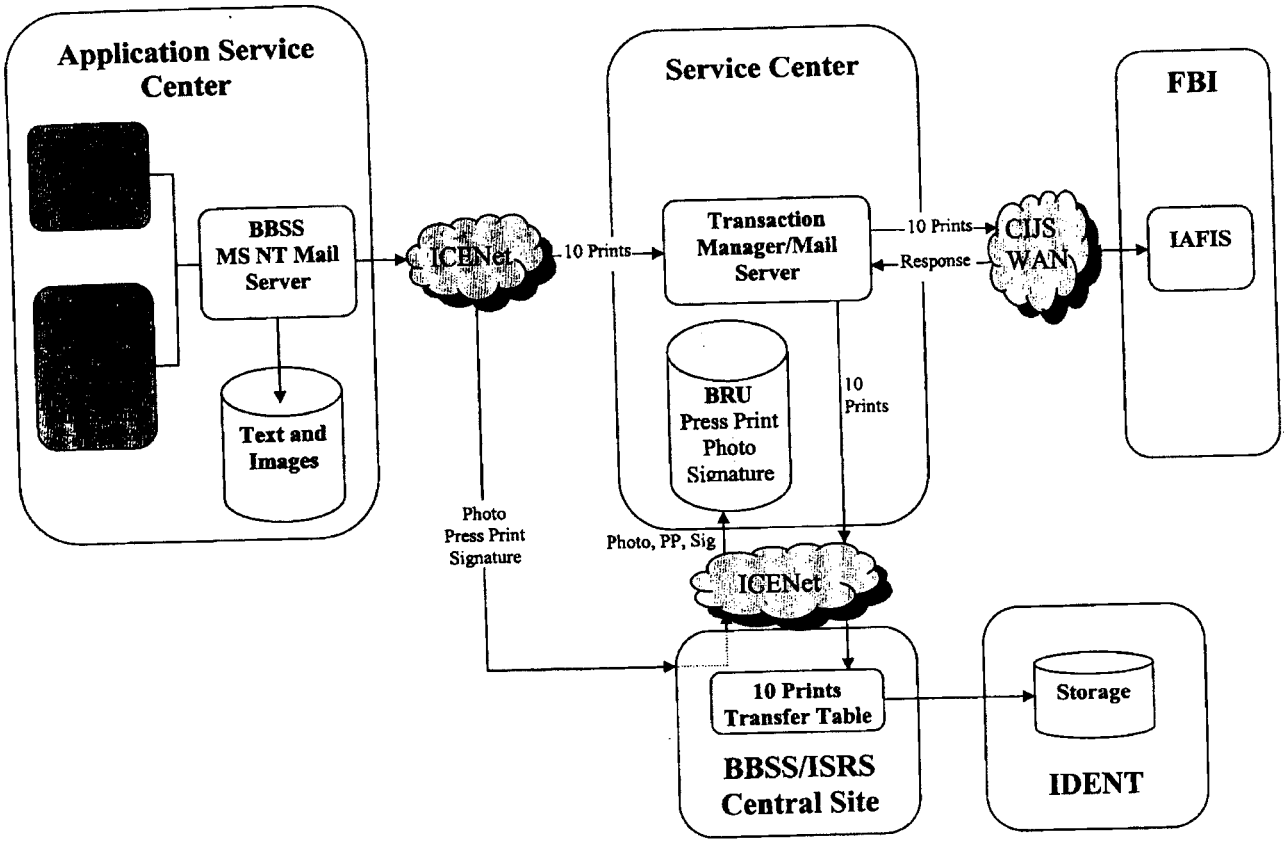
Dell PowerEdge Server (typically 2950)
4 GB RAM
8 GB Hot Swappable RAID 5 storage (at least 14GB at larger ASCs)
CD-ROM
100 Base-T NIC
Monitor

Data Storage Requirements:

ASC Size:

Largest ASC	7GB
Medium ASC	4GB
Smallest ASC	<1GB

USCIS – BIOMETRICS CAPTURE



Live-Scan Deployment Schedule

Type	Site Name	Site Code	Address	City	ST	Zip	Cabinet	Desk top	Mobile	Total to be Installed	Day	Notes
				Detroit	MI	48214-3332	4	1	1	5	1 & 2	
COLO	Detroit	XDK	11411 East Jefferson Ave	Boston	MA	02114-1706	2		1	7	1 & 2	
SA	Boston	XDD	115 Federal St									
				Lawrence	MA	01840-1602	2	1		3	3	
COLO	Lawrence	XBK	2 Mill Street	Kentwood	MI	49508-5270	2	1	1	3	3	
SA	Grand Rapids	XDM	4494 Breton Rd									
				Cranston	RI	02920-5568	3		1	3	4	
SA	Providence	XEF	100 Sockanosset Cross Rd, Suite 230	Cleveland	OH	44199-2065	2		1	2	4 & 5	
COLO	Cleveland	XCH	1240 E.9th St. Room 1258									
				Merrillville	IN	46410-2265	2			2	5	
COLO	Merrillville	XBG	518 Clark St									
		# SITES Scheduled WK 1 - 12	3 North East Region 3 South East Region 3 Central Region 3 Western Region	Total # sites Scheduled to date	12				# Machies installed WK 1	45	CUMMULATIVE	45
				South Portland	ME	04106-6909	2			2	6	
COLO	Portland, ME	XBJ	178 Gannett Drive	Columbus	OH	43215-6903	2		1	2	6	
SA	Columbus	XCK	50 W. Broad St. Suite 650									
				Buffalo	NY	14202-2698	2		1	2	7	
COLO	Buffalo	XBH	1300 Ellicott Street	Cincinnati	OH	45202-5298	2		1	2	7	
COLO	Cincinnati	XCJ	550 Main St. Room 1524	Latham	NY	12110-1024	2			2	8	
COLO	Albany	XBI	1058 Troy-Schenectady Rd	Louisville	KY	40202-2250	2		1	2	8	
COLO	Louisville	XNF	601 W. Broadway, Room 22	St Albans	VT	05478-9500	1	1		2	9	
COLO	St Albans, VT	XPK	64 Gilcebrook Dr	Indianapolis	IN	46204-3915	2			2	9	
COLO	Indianapolis	XCG	950 N. Meridian St. Room 400									
				East Hartford	CT	06118-1104	3		1	3	10	
SA	Hartford	XBE	457 Silver Lane	Michigan City	IN	46360-7340	2	1	1	3	10 & 11	
SA	Michigan City	XCF	284 Dunes Plaza					1			10 & 11	
		# SITES Scheduled WK 2 - 15	5 North East Region 3 South East Region 5 Central Region 2 Western Region	Total # sites Scheduled to date	27				# Machines Installed Wk 2	48	CUMMULATIVE	93
COLO	Syracuse	XBJ	412 S. Warren St	Syracuse	NY	13202-2604	2			2	11	
				Norridge	IL	60706-2905	3	1	1	4	12 & 13	
SA	Norridge	XCA	4701 N. Cumberland, 1-3 BCD	New Rochelle	NY	10801-6405	4	1	1	5	12 & 13	
SA	New Rochelle	XNG	268 North Ave									
				Chicago	IL	60632-4263	3	1	1	4	14 & 15	
SA	Pulaski	XCB	5100 S. Pulaski Rd, Suite 101									
				Brooklyn	NY	11219-4929	9	1	1	10	14 & 15	
SA	Brooklyn	XNI	1260-1276 60th St									
		# Sites Scheduled WK 3 - 10	3 North East Region 2 South East Region 2 Central Region 3 Western Region	Total # sites Scheduled to date	37				# Machines Installed WK 3	47	CUMMULATIVE	140
				Chicago	IL	60640-3603	3	1	1	4	16 & 17	
SA	Broadway	XCC	4953 N. Broadway	Bronx	NY	10473-3017	5	1	1	6	16 & 17	
SA	Bronx	XNJ	1621 Westchester Ave									
				Naperville	IL	60540-0982	3	1	1	4	18 & 19	
SA	Naperville	XCD	888 South Route 59, Suite 124									

Live-Scan Deployment Schedule

Type	Site Name	Site Code	Address	City	ST	Zip	Cabinet	Desk top	Mobile	Total to be Installed	Day	Notes
COLO	Manhattan	XNK	201 [illegible]	New York	NY	10011-4311	7	1		8	18 & 19	
SA	Waukegan	XCE	25 S. Greenbay Rd	Waukegan	IL	60085-4815	2	1	1	3	20 & 21	
SA	Hicksville (Heimstead)	XNL	81 Broadway Road	Hicksville	NY	11801-1503	4		1	4	20 & 21	
		# Sites Scheduled WK 4 - 12	3 North East Region 3 South East Region 3 Central Region 3 Western Region	Total # sites Scheduled to date	49				WK 4	59	CUMMULATIVE	199
COLO	Milwaukee	XCH	310 E. Knapp St. Room 154	Milwaukee	WI	53202-4504	3			3	22	
SA	Queens	XNM	15-01 Jamaica Ave	Jamaica	NY	11432-4910	5	2		7	22 & 23	
SA	St. Paul	XSI	1360 University Ave	St. Paul	MN	55104-4066	3	1	1	4	23 & 24	
SA	Woodside	XNN	61-05 Roosevelt Ave	Woodside	NY	11377-3551	5	1	1	7	24 & 25	
COLO	Duluth	XSM	515 W. First St. Suite 208	Duluth	MN	55802-1301	1	1		2	25 & 26	
		# Sites Scheduled WK 5 - 10	2 North East Region 2 South East Region 3 Central Region 3 Western Region	Total # sites Scheduled to date	59				WK 5	39	CUMMULATIVE	238
SA	Elizabeth	XND	295 North Broad St	Elizabeth	NJ	07208-2303	11	1	1	12	26 & 27 & 28	
COLO	Fargo	XSK	657 2nd Ave. North, Room #248	Fargo	ND	58102-4727	1	1		2	27 & 28	
SA	Hackensack	XNP	116 Kansas Street, Main Floor	Hackensack	NJ	07601-7103	3		1	3	28 & 29	
SA	Rapid City	XSJ	2255 Haines Ave, Suite 214	Rapid City	SD	57701-0411	1	1		2	29 & 30	
SA	Philadelphia	XPA	10300 Drummond Rd, Suite 100	Philadelphia	PA	19154-3804	6	1	1	7	30 & 31	
		# Sites Scheduled WK 6 - 10	3 North East Region 3 South East Region 2 Central Region 2 Western Region	Total # sites Scheduled to date	69				WK 6	46	CUMMULATIVE	284
COLO	Sioux Falls	XSL	300 E. 8th St	Sioux Falls	SD	57103-7023	1	1		2	31 & 32	
SA	Pittsburgh	XPB	600 Grant St, Suite 101	Pittsburgh	PA	15219-2805	2		1	2	32	
COLO	Charleston, WV	XRC	210 Kanawha Boulevard West	Charleston	WV	25302-2201	1	1		2	33	
COLO	Des Moines	XOB	210 Walnut St. Room 849	Des Moines	IA	50309-2110	2		1	2	33 & 34	
SA	Dover	XPD	280 [illegible] South Bay, Suite 220 & 270	Dover	DE	19901-7008	1		1	2	34	
COLO	York	XPE	340 Concord Ave, Old Farm House	York	PA	17402-2007	2			2	35	
COLO	Omaha	XOA	1717 Avenue H	Omaha	NE	68110-2752	2			2	35 & 36	

Live-Scan Deployment Schedule

Type	Site Name	Site Code	Address	City	ST	Zip	Cabinet	Desk top	Mobile	Total to be Installed	Day	Notes
		# Sites Scheduled WK 7 - 13	4 North East Region 3 South East Region 3 Central Region 3 Western Region	Total # sites Scheduled to date	82				WK 7	36	CUMMULATIVE	320
SA	Baltimore	XBA	100 South Charles St, Suite 701	Baltimore	MD	21201-2701	4	1	1	5	36 & 37	
COLO	Kansas City	XKA	9747 N. Conant Ave	Kansas City	MO	64153-1833	2	1	1	3	37 & 38	
SA	Glen Burnie	XBB	1243 [illegible] Crain Highway Plaza, Suite G	Glen Burnie	MD	21061-3546	4	1	1	5	38 & 39	
COLO	St. Louis	XKC	1222 Spruce St Room 1.206	St. Louis	MO	63103-2815	2	1	1	3	39 & 40	
SA	Salisbury	XBC	2040 Shockley Drive Suite C2	Salisbury	MD	21801-7674	1	1	1	2	40	
		# Sites Scheduled WK 8 - 9	3 North East Region 2 South East Region 2 Central Region 2 Western Region	Total # sites Scheduled to date	91				WK 8	36	CUMMULATIVE	356
COLO	Wichita	XKB	271 W. 3rd St. North, Suite 1050	Wichita	KS	67202-1212	1	1		2	41 & 42	
SA	Dulles	XDE	3050 Centreville Hwy, Suite 100	Dulles	VA	20190-1560	6	1	1	9	41 & 42 & 43	
SA	Denver	XDG	15037 E. Colfax Ave. Unit G	Aurora	CO	80011-5777	4	1	1	5	42 & 43	
SA	Dallas North	XDA	10051 Whitehurst Dr, Suite 200	Dallas	TX	75243-0837	4	1	1	5	43 & 44	2nd Central Team
SA	Norfolk	XDF	2560 Almeda Ave, Suite 114	Norfolk	VA	23513-2503	2		1	2	44	
SA	Grand Junction	XDH	2454 Hwy 6 and 50, Valley Plaza, Suite 115	Grand Junction	CO	81505-1111	1	1	1	2	44 & 45	
SA	Dallas South	XDL	7334 South Westmoreland Rd	Dallas	TX	75237-2908	2	1	1	3	45	2nd Central Team
		# Sites Scheduled WK 9 - 12	2 North East Region 1 South East Region 5 Central Region 4 Western Region	Total # sites Scheduled to date	103				WK 9	48	CUMMULATIVE	404
SA	Ft Worth	XDB	4200 S. Freeway, Suite 1309	Ft Worth	TX	76115-1400	3	1	1	4	46	2nd Central Team
SA	Salt Lake City	XDJ	5538 S. 1900 West St. Bldg C	Taylorsville	UT	84118-9007	2	1	1	3	46 & 47	
SA	Lubbock	XDC	3502 Slide Rd, Suite A-24	Lubbock	TX	79414-2547	2		1	2	47 & 48	2nd Central Team
COLO	Casper	XDI	150 East B St. Room 1014	Casper	WY	82601-7005	1	1		2	48 & 49	
COLO	Oklahoma	XDD	4400 S.W. 44th St. Suite A	Oklahoma City	OK	73119-2800	2		1	2	49 & 50	2nd Central Team
SA	Idaho Falls	XHE	2285 W. Broadway, Suite A	Idaho Falls	ID	83402-2996	1	1	1	2	50 & 51	
		# Sites Scheduled WK 10 - 9	6 Central Region 3 Western Region	Total # sites Scheduled to date	112				WK 10	32	CUMMULATIVE	436
SA	Houston SE	XHH	10555 Northwest Freeway, Suite 150	Houston	TX	77092-8209	3	2	1	5	51 & 52	2nd Central Team
COLO	Boise	XHD	1185 South Vinnell Way	Boise	ID	83709-1656	1	1		2	52 & 53	
SA	Houston NW	XHI	10555 Northwest Freeway, Suite 150	Houston	TX	77092-8209	4		1	4	53 & 54	2nd Central Team
COLO	Helena	XHC	2900 Skyway Dr	Helena	MT	59602-1230	1	1		2	54 & 55	
SA	Houston SW	XHI	11777 State Hwy 6 South	Sugar Land	TX	77498-5721	4	1	1	5	55 & 56	2nd Central Team

HSSCCG-10-J-00034 Attachment D

Live-Scan Deployment Schedule

Type	Site Name	Site Code	Address	City	ST	Zip	Cabinet	Desk top	Mobile	Total to be Installed	Day	Notes
		# Sites Scheduled WK 11 - 8	5 Central Region 3 Western Region	Total # sites Scheduled to date	120				WK 11	25	CUMMULATIVE	461
SA	Austin	XSN	Parkline Plaza Shopping Center 11301 Lakeline Blvd. Suite 150	Austin	TX	78717	2	1	1	3	57 & 58	2nd Central Team
SA	San Antonio	XSA	5121 Crestway, Suite 112	San Antonio	TX	78239-1975	3	1	1	4	59 & 60	2nd Central Team
SA	Laredo	XJX	707 E. Calton Rd. Suite 301	Laredo	TX	78041-3638	3		1	3	60 & 61	2nd Central Team
		# Sites Scheduled WK 12 - 6	3 Central Region 3 Western Region	Total # sites Scheduled to date	126				WK 12	22	CUMMULATIVE	483
SA	McAllen	XHA	220 South Bicentennial, Suite C	McAllen	TX	78501-7051	2	1	1	3	62 & 63	2nd Central Team
COLO	Harlingen	XHB	1717 Zoy St	Harlingen	TX	78552-3220	2			2	64 & 65	2nd Central Team
		# Sites Scheduled WK 13 - 3	2 Central Region 1 Western Region	Total # sites Scheduled to date	129				WK 13	7	CUMMULATIVE	490
SA	El Paso	XEA	10500 Montwood	El Paso	TX	79935-2703	3		1	3	66 & 67	2nd Central Team
SA	Albuquerque	XEC	1605 Iaiete Blvd SW, Suite C	Albuquerque	NM	87105-4793	2		1	2	68 & 69	2nd Central Team
		# Sites Scheduled WK 14 - 3	2 Central Region 1 Western Region Goleta is proposed for closure	Total # sites Scheduled to date	132				WK 14	7	CUMMULATIVE	497
			NORTHEAST REGION									
			SOUTH EAST REGION									
			CENTRAL REGION									
			WESTERN REGION									

Type	Site Name	Site Code	Address	City	ST	Zip	Cabinet	Desktop	Mobile	Total to be Installed	Number of Days	Day	Notes
							INSTALL	INSTALL	STORE				
NORTHEAST REGION													
DISTRICT 1													
SA	Boston	XBD	170 Portland St	Boston	MA	02114-1706	7		1	7	2	Day 1 & 2	
SA	Providence	XBF	105 Sockanosset Cross Rd, Suite 210	Cranston	RI	02920-5560	3		1	3	1	Day 4	
COLO	Manchester	XBG	803 Canal St	Manchester	NH	03101-1226	2			2	1	Day 5	
DISTRICT 2													
COLO	Buffalo	XBH	130 Delaware Ave	Buffalo	NY	14202-2496	2		1	2	1	Day 7	
COLO	Albany	XBI	1086 Troy-Schenectady Hwy	Latham	NY	12110-1024	2			2	1	Day 8	
SA	Hartford	XBE	467 Silver Lane	East Hartford	CT	06118-1104	3		1	3	1	Day 10	
COLO	Syracuse	XBJ	412 S. Warren St	Syracuse	NY	13202-2604	2			2	1	Day 11	
DISTRICT 3													
SA	New Rochelle	XNG	246 North Ave	New Rochelle	NY	10801-6405	4	1	1	5	1	Day 12 & 13	
SA	Brooklyn	XNI	1260-1278 60th St	Brooklyn	NY	11219-4928	9	1	1	10	3	Day 14 & 15	
SA	Bronx	XNJ	1827 Westchester Ave	Bronx	NY	10472-3017	5	1	1	6	2	Day 16 & 17	
COLO	Manhattan	XNK	201 W Houston St. Street Entrance send mail & DHL to 201 Varick St. Suite 1023	New York	NY	10014-4811	7	1		8	2	Day 18 & 19	
SA	Hicksville (Hemostead)	XNL	87 Bethpage Road	Hicksville	NY	11801-1503	4		1	4	1	Day 20 & 21	
SA	Queens/ Jamaica	XNM	153-01 Jamaica Ave	Jamaica	NY	11432-4910	5	2		7	2	Day 22 & 23	
SA	Woodside	XNN	63-05 Roosevelt Ave	Woodside	NY	11377-3641	6	1	1	7	2	Day 24 & 25	
DISTRICT 4													
SA	Elizabeth	XNO	265 North Broad St	Elizabeth	NJ	07208-2303	11	1	1	12	3	Day 26 & 27 & 28	
SA	Hackensack	XNP	116 Kansas Street, Main Floor	Hackensack	NJ	07601-7103	3		1	3	1	Day 29	
DISTRICT 5													
SA	Philadelphia	XPA	10300 Drummond Rd, Suite 100	Philadelphia	PA	19154-3804	6	1	1	7	2	Day 30 & 31	
SA	Pittsburgh	XPB	800 Penn Ave, Suite 101	Pittsburgh	PA	15222-3615	2		1	2	1	Day 32	
SA	Dover	XPD	250 Gateway South Blvd, Suites: 260 & 270	Dover	DE	19901-4699	1	1	1	2	1	Day 34	
COLO	York	XPE	3400 Concord Rd, Old Farm House	York	PA	17402-9007	2			2	1	Day 35	
DISTRICT 6										1			
SA	Baltimore	XBA	100 South Charles St, Suite 201	Baltimore	MD	21201-2701	4	1	1	5	2	Day 36 & 37	
SA	Glenmont	XBB	12331 Georgia Ave, Glenmont Plaza, Suite C	Wheaton	MD	20906-3646	4	1	1	5	2	Day 38 & 39	
DISTRICT 7													
SA	Alexandria	XDE	8850 Richmond Hwy, Suite 100	Alexandria	VA	22309-1586	8	1	1	9	3	Day 41 & 42 & 43	
SA	Norfolk	XDF	2500 Almeda Ave, Suite 114	Norfolk	VA	23513-2503	2		1	2	1	Day 44	
							111	17		128	44		
SOUTHEAST REGION													

HSSCCG-10-J-00034 - ATTACHMENT E

UKvisas Software Requirements

1 Background

UKvisas has embarked on a global rollout of biometric capabilities to record fingerprints and photographs for all UK visa applicants (with limited exceptions and exemptions) since December 2008. This element of the application process requires visa applicants to physically present themselves so their biometrics can be recorded. UKvisas has been aware of the network of Department of Homeland Security (DHS) Application Support Centers (ASCs) in place for similar biometric recording for US immigration purposes.

In September 2006, Tony Mercer, Director UKvisas Network Operations, formally wrote to Stewart Baker, DHS Assistant Secretary for Policy, requesting formal exploration and analysis for UKvisas use of the ASCs for UK visa applicants to appear for fingerprinting and photograph recording.

In November 2006, Stewart Baker responded positively with agreement to conduct a joint feasibility or viability report considering the legal, policy, cost, technical, and operational factors as a determination and basis for future agreements for UKvisas use of the ASCs.

A joint viability report has been concluded between UKvisas and DHS as agreed to in above referenced letters. The viability report analysis has identified significant benefits for DHS and UKvisas through the use of ASCs and the data sharing opportunities this presents. Both UKvisas and DHS have committed to the implementation of Phase 1a identified in the viability report by November 30, 2007. Phase 1a includes the joint enrolment capabilities for UK visa applicants to appear at ASCs for biometric enrolment and the data being transmitted by DHS to UKvisas.

2 UKvisas Software Requirements

2.1 Introduction

The Live-Scan software is to: 1) include a screen to be used for processing UKvisas applicants, 2) include required data fields necessary for submitting UKvisas applicant information, 3) capture digital photographs, and 4) be capable of recording and enrolling all the data necessary for submission to the UK Immigration and Asylum Fingerprint System (IAFS).

The ASC enrolment software must be capable of enrolling the following data for UK visa applicants age five (5) and older:

- UKvisas Global Web Form (GWF) number

- Minimum enrolment set (family name, other names, date of birth, sex, passport number, and nationality)
- Exemption/Exception details
- Fingerprints
- Digital photo
- Audit data

The following requirements will need to be satisfied in the development of the ASC software for processing UK visa applicants.

2.2 General Requirements

R1 Biometric recording shall be record-centric. For each applicant the operator shall be able to create a new biometric submission file to be populated with biometrics and biographic data.

R2 The operator shall have capability to cancel or void a record at any stage prior to confirmation and submission of the record.

R3 Only one record shall be open at one time per ASC workstation.

R4 When the enrolment set is complete the software shall prompt the operator to confirm that they are content for the data set to be submitted. Once the operator has confirmed the software shall lock the record and begin the process for transmitting data to UKvisas.

R5 The software shall not allow the biometric or biographic details to be edited or accessed once confirmed by the operator.

R6 Each record shall be date/time stamped on creation. Standard format and time zone for date/time stamp to be agreed between UKvisas and DHS.

R7 The software shall allow for the creation of metadata relating to each enrolment set. Examples include the enrolment post, the enrolment workstation, the operator's log on ID, time stamp etc. This data will be used for Management Information (MI) purposes as well as for IAFIS and is identified in detail in later sections.

R8 In the event that a network connection is not available, the software shall be capable of locally storing records in a secure manner.

R9 The software shall submit all locally stored records immediately following a network connection being re-established.

R10 The software shall allow operators to re-take fingerprints where necessary prior to submission, but only up until the point the operator confirms the record to lock and submit the data.

R11 The software shall have capability to identify and flag the record as an UK visa applicant for appropriate processing different than DHS applicants.

2.3 Login Requirements

UKvisas accepts that the current requirements for the ASC personnel to login and authenticate their use of the software are more than likely adequate, however UKvisas desires the following minimal requirements are met:

R12 The software shall restrict access to its function to operators that successfully authenticate themselves by username and password.

R13 All actions by system administrators regarding UKvisas records shall be logged for auditing purposes.

2.4 Minimum Data Set Entry Requirements

R14 The software shall accept the minimum data set for biometric enrolment including GWF, Family name, Other Names, Date of Birth, Sex, Travel Document Number, and Nationality.

R15 The software shall allow for manual data entry of the minimum data set.

R16 The software shall allow for entry of the minimum data set via a 2D bar code reader using PDF417 standard.

R17 All fields of the minimum enrolment set listed in R14 shall be mandatory with the exception of "Other Names," which is optional.

The following chart provides an overview of the biographic data entry requirements as detailed in the next sub sections.

Field Name	Condition	Size	Permissible Values
GWF Number	Mandatory	12	"GWF" followed by 9 unique numeric characters
Family Name	Mandatory	1-35	Alphabetical and special characters
Other Names	Optional	0-35	Alphabetical and special characters
Date of Birth	Mandatory	8	MMDDCCYY format
Sex	Mandatory	1	M, F, or U only
Nationality	Mandatory	3	List of country codes provided by UKvisas
Travel Document Number	Mandatory	1-15	Any alphabetical, numeric, or special characters.
Exemption/ Exception	Optional	1	Available values: 1 – Amputee (less than two fingers available) 2 - Medically Incapable

Table 1: Summary of Biographic Data Requirements

2.4.1 GWF Entry Requirements

R18 The software shall accept by reading from bar code or by manual entry the GWF number generated by visa4uk in the format of 12 alphabetical and numeric characters.

R19 The GWF shall always be in format of the GWF followed by 9 numeric characters (e.g., GWF123456789).

R20 Operators shall have capability to edit GWFs in case of incorrect data or misreads from bar code until the record is confirmed.

R21 The GWF field shall be a mandatory field.

R22 Intelligence shall be placed on the field to verify the length and format of any GWF entered into the software as stated in R19.

2.4.2 Family Names

The software shall accept by reading from bar code or by manual entry the Family Names as shown on the UK visa applicant's valid travel document (Note: last names in U.S. terms or Surnames usually shown on most passports).

R23 The length and format of the Family Names field shall be any alphabetical or special characters with minimum of 1 character and maximum of 35 characters.

R24 Operators shall have capability to edit Family Names in case of incorrect data or misreads from bar code until the record is confirmed.

R25 The Family Names field shall be a mandatory field.

R26 Intelligence shall be placed on the field to verify the length and format of any Family Names entered into the software as stated in R24.

2.4.3 Other Names

The software shall accept by reading from bar code or by manual entry the Other Names as shown on the UK visa applicant's valid travel document (Note: combination of first and middle names in U.S. terms or given names usually shown on most passports).

R27 The length and format of the Other Names field shall be any alphabetical or special characters with minimum of 0 characters and maximum of 35 characters.

R28 Operators shall have capability to edit Other Names in case of incorrect data or misreads from bar code until the record is confirmed.

R29 The Other Names field shall be an optional field.

R30 Intelligence shall be placed on the field to verify the length and format of any Other Names entered into the software as stated in R29.

2.4.4 Date of Birth

The software shall accept by reading from bar code or by manual entry the Date of Birth as shown on the UK visa applicant's valid travel document.

R31 The length and format of the Date of Birth field shall be any numeric character 8 characters in format of MMDDCCYY (e.g., 12201976).

R32 Operators shall have capability to edit Date of Birth field in case of incorrect data or misreads from bar code until the record is confirmed.

R33 The Date of Birth field shall be a mandatory field.

R34 Intelligence shall be placed on the field to verify the length and format of any Date of Birth entered into the software as stated in R31.

R35 Intelligence shall be available on the date of birth field to identify those applicants who are below the age of 5 years.

R36 Where a child under the age of 5 years has been identified, the software shall provide a message to the operator informing that the child is not required to be enrolled and not allow operator to continue with the enrolment.

2.4.5 Sex

R37 The software shall accept by reading from bar code or by manual entry the Sex as shown on the UK visa applicant's valid travel document.

R38 The length and format of the Sex field shall be 1 character with "M," "F," or "U" as the only allowable characters.

R39 Operators shall have capability to edit Sex field in case of incorrect data or misreads from bar code until the record is confirmed.

R40 The Sex field shall be a mandatory field.

R41 Intelligence shall be placed on the field to verify the length and format of any Sex entered into the software as stated in R38.

2.4.6 Nationality

The software shall accept by reading from bar code or by manual entry the Nationality as shown on the UK visa applicant's valid travel document.

R42 The length and format of the Nationality field shall be 3 alphabetical characters and allowable Nationality codes are available in Appendix A.

R43 Operators shall have capability to edit Nationality field in case of incorrect data or misreads from bar code until the record is confirmed.

R44 The Nationality field shall be a mandatory field.

R45 Intelligence shall be placed on the field to verify the length and format of any Nationality entered into the software as stated in R42.

2.4.7 Travel Document Number

The software shall accept by reading from bar code or by manual entry the Travel Document Number as shown on the UK visa applicant's valid travel document.

R46 The length and format of the Travel Document Number field shall be any alphabetical, numeric, or special characters with minimum of 1 character and maximum of 15.

R47 Operators shall have capability to edit Travel Document Number field in case of incorrect data or misreads from bar code until the record is confirmed.

R48 The Travel Document Number field shall be a mandatory field.

R49 Intelligence shall be placed on the field to verify the length and format of any Travel Document Number entered into the software as stated in R46.

2.4.8 Exemptions/Exceptions

The operator shall have capability to select an exemption/exception for two cases: 1) Amputee with less than two fingers of the middle 8 fingers available (middle 8 fingers are defined as all fingers and thumbs excluding the little fingers); or 2) Physically unable to provide fingerprints (e.g., severe arthritis).

R50 The supervisor approval capability shall have ability to disallow exemption/exception returning the use to the normal workflow.

2.5 Fingerprint Enrolment Requirements

The software shall be capable of recording up to 10 individual rolled fingerprint images.

R51 The software shall be capable of recording up to 4 slap fingerprint images consisting of up to 4 left fingers, up to 4 right hand fingers, right thumb, and left thumb.

R52 The software shall have capability to measure quality of fingerprints images recorded.

R53 The software shall have capability to inform operator when desired quality measurement has not been achieved to re-take images to improve quality.

R54 The software shall have capability to allow operator to re-take fingerprints images until an acceptable quality threshold is met or operator determines the best quality possible has been recorded.

R55 The software shall have capability to record a date/time stamp at the point when all fingerprints have been successfully recorded. Standard format and time zone for date/time stamp to be agreed between UKvisas and DHS.

R56 The system shall display the fingerprint images to the operator for visual review.

R57 The software shall have capability to perform a sequence check to ensure rolled images are in proper order.

R58 The software shall have capability to allow operators to identify missing fingers (e.g., amputees), bandaged, or permanently damaged (e.g., scars/deformity).

R59 All fingerprints images shall be compressed using Wavelet Scalar Quantisation (WSQ) 15:1 ratio.

2.6 Digital Photograph Enrolment Requirements

R60 The system shall record a digital facial image of the UK visas applicant with goal of meeting International Civil Aviation Organisation (ICAO) compliance standards, however the measurement of ICAO compliance is NOT required. Best practices for photograph capture shall be implemented from ICAO such as no hats, no smiling, full frontal with minimal horizontal or vertical misalignment, etc.

R61 The system shall record a date/time stamp at the point when photo is taken. Standard format and time zone for date/time stamp to be agreed between UKvisas and DHS.

R62 The system shall record a true rendition of the image collected free from image enhancement or resolution mapping.

R63 The software shall display the image to the operator to perform a visual check of the image.

R64 The operator shall be allowed to cancel or re-take an image capture without cancelling or deleting the entire record.

3 Transmission of Data from ASCs to UKvisas Requirements

The following requirements are for the transmission of the data from DHS ASCs to UKvisas in the Phase 1a of the project.

R65 The biometric and biographic data for each UK visa applicant shall be provided in the FBI Electronic Fingerprint Transmission Specification (EFTS) by DHS to UKvisas.

R66 The EFTS file with contain for each visa applicant (1) Type-1 record (message header), one (1) Type-2 record (biographical, demographic, etc. data), up to 14 Type-4 records (10 individual rolled images and 4 slap images), and one (1) Type-10 record (digital photograph).

R67 The EFTS file shall be transmitted as e-mail attachments using Simple Mail Transfer Protocol (SMTP) over a secure Internet connection between DHS and UKvisas.

R68 The EFTS file shall be delivered to UKvisas within 12 hours of the completion of the biometric enrolment process at the ASCs.

R69 DHS shall temporarily retain the EFTS file until USCIS confirms successful delivery of the file using native SMTP capabilities.

R70 After successful delivery of EFTS file, UKvisas shall return a receipt notification to DHS for deletion of the files.

R71 Upon successful receipt, UKvisas will translate the EFTS records to Extensible Markup Language (XML) based records required for submittal to IAFS.

R72 The EFTS files shall include the following fields with mandatory and optional fields marked appropriately. Additional fields may be added at later date based on discussions between DHS and UKvisas.

1. Unique ID (Mandatory)
2. Family Name (Mandatory)
3. Other Names (Optional)
4. Date of Birth (Mandatory)
5. Sex (Mandatory)
6. Nationality (Mandatory)
7. Travel Document Number (Mandatory)
8. Exemption/Exception Code (Optional – default could be null)
9. ASC Location (Mandatory)
10. Workstation ID (Mandatory)
11. Operator ID (Mandatory)
12. Fingerprint Scanner ID (Optional)
13. Camera ID (Optional)
14. Fingerprint Recording Completion Date/Time Stamp (Mandatory)
15. Photograph Recording Completion Date/Time Stamp (Mandatory)
16. Fingerprint Presence for Each Finger (Mandatory)
17. WSQ Compressed Fingerprint Images (Mandatory for all available fingers)
18. Fingerprint Image Horisontal Line Length (Mandatory)
19. Fingerprint Image Vertical Line Length (Mandatory)
20. Photograph (Mandatory)
21. Photograph Width (Mandatory)
22. Photograph Length (Mandatory)
23. Quality Control (QC) ID (Optional)

Appendix A: Nationality Codes

CODE	NATIONALITY
AFG	AFGHANISTAN
ALB	ALBANIA
DZA	ALGERIA
ASM	AMERICAN SAMOA
AND	ANDORRA
AGO	ANGOLA
ATG	ANTIGUA AND BARBUDA
ARG	ARGENTINA
ARM	ARMENIA
ABW	ARUBA
AUS	AUSTRALIA
AUT	AUSTRIA
AZE	AZERBAIJAN
BHS	BAHAMAS
BHR	BAHRAIN
BGD	BANGLADESH
BRB	BARBADOS
BLR	BELARUS
BEL	BELGIUM
BLZ	BELIZE
BEN	BENIN
BTN	BHUTAN
BOL	BOLIVIA
BIH	BOSNIA AND HERZEGOVINA
BWA	BOTSWANA
BVT	BOUVET ISLAND
BRA	BRAZIL
GBR	GREAT BRITAIN
VGB	BRITISH VIRGIN ISLANDS
BRN	BRUNEI DARUSSALEM
BGR	BULGARIA
BFA	BURKINA FASO
BDI	BURUNDI
CMR	CAMEROON
CAN	CANADA
CPV	CAPE VERDE
CAF	CENTRAL AFRICAN REPUBLIC
TCD	CHAD
CHL	CHILE
CHN	CHINA
CXR	CHRISTMAS ISLAND
CCK	COCOS (KEELING) ISLANDS
COL	COLOMBIA
COM	COMOROS
COG	CONGO
COD	CONGO (DEMOCRATIC REP OF)
COK	COOK ISLANDS
CRI	COSTA RICA
CIV	COTE D'IVOIRE (IVORY COAST)
HRV	CROATIA

CODE	NATIONALITY
CUB	CUBA
CYP	CYPRUS
CZE	CZECH REPUBLIC
DNK	DENMARK
DJI	DJIBOUTI
DMA	DOMINICA
DOM	DOMINICAN REPUBLIC
ECU	ECUADOR
EGY	EGYPT
SLV	EL SALVADOR
GNQ	EQUATORAL GUINEA
ERI	ERITREA
EST	ESTONIA
ETH	ETHIOPIA
FJI	FIJI
FIN	FINLAND
FRA	FRANCE
GUF	FRENCH GUIANA
FXX	FRENCH METROPOLITAN
PYF	FRENCH POLYNESIA
ATF	FRENCH SOUTHERN TERRITORIES
GAB	GABON
GMB	GAMBIA
GEO	GEORGIA
D	GERMANY
GHA	GHANA
GRC	GREECE
GRL	GREENLAND
GRD	GRENADA
GLP	GUADELOUPE
GUM	GUAM
GTM	GUATEMALA
GIN	GUINEA
GNB	GUINEA-BISSAU
GUY	GUYANA
HTI	HAITI
HMD	HEARD AND MCDONALD ISLANDS
VAT	HOLY SEE (VATICAN CITY STATE)
HND	HONDURAS
HKG	HONG KONG SPECIAL ADMINISTRATIVE REGION OF CHINA
HUN	HUNGARY
ISL	ICELAND
IND	INDIA
IDN	INDONESIA
IRN	IRAN
IRQ	IRAQ
IRL	IRELAND
ISR	ISRAEL
ITA	ITALY
JAM	JAMAICA
JPN	JAPAN
JOR	JORDAN
KHM	KAMPUCHEA

CODE	NATIONALITY
KAZ	KAZAKHSTAN
KEN	KENYA
KIR	KIRIBATI
UNK	KOSOVO RESIDENT - UN ISSUED TRAVEL DOCUMENT
KWT	KUWAIT
KGZ	KYRGYZSTAN
LAO	LAOS
LVA	LATVIA
LBN	LEBANON
LSO	LESOTHO
LBR	LIBERIA
LBY	LIBYA
LIE	LIECHTENSTEIN
LTU	LITHUANIA
LUX	LUXEMBOURG
MAC	MACAO SPECIAL ADMINISTRATIVE REGION OF CHINA
MKD	MACEDONIA (FORMER YUGOSLAV REP OF)
MDG	MADAGASCAR
MWI	MALAWI
MYS	MALAYSIA
MDV	MALDIVES
MLI	MALI
MLT	MALTA
MHL	MARSHALL ISLANDS
MTQ	MARTINIQUE
MRT	MAURITANIA
MUS	MAURITIUS
MYT	MAYOTTE
MEX	MEXICO
FSM	MICRONESIA (FEDERATED STATES OF)
MDA	MOLDOVA (REP OF)
MCO	MONACO
MNG	MONGOLIA
MAR	MOROCCO
MOZ	MOZAMBIQUE
MNE	REPUBLIC OF MONTENEGRO
MMR	MYANMAR
NAM	NAMIBIA
NRU	NAURU
NPL	NEPAL
NLD	NETHERLANDS
ANT	NETHERLANDS ANTILLES
NCL	NEW CALEDONIA
NZL	NEW ZEALAND
NIC	NICARAGUA
NER	NIGER
NGA	NIGERIA
NIU	NIUE
NFK	NORFOLK ISLAND
PRK	NORTH KOREA (DEMOCRACTIC PEOPLE'S REP OF)
MNP	NORTHERN MARIANA ISLANDS
NOR	NORWAY
OMN	OMAN

CODE	NATIONALITY
PAK	PAKISTAN
PLW	PALAU
PSE	PALESTINIAN AUTHORITY
PAN	PANAMA
PNG	PAPUA NEW GUINEA
PRY	PARAGUAY
PER	PERU
PHL	PHILIPPINES
POL	POLAND
PRT	PORTUGAL
PRI	PUERTO RICO
QAT	QATAR
XXB	REFUGEE - ARTICLE 1 OF THE 1951 CONVENTION
REU	REUNION
ROU	ROMANIA
RUS	RUSSIAN FEDERATION
RWA	RWANDA
WSM	SAMOA
SMR	SAN MARINO
STP	SAO TORME AND PRINCIPE
SAU	SAUDI ARABIA
SEN	SENEGAL
SRB	REPUBLIC OF SERBIA
SYC	SEYCHELLES
SLE	SIERRA LEONE
SGP	SINGAPORE
SVK	SLOVAKIA
SVN	SLOVENIA
SLB	SOLOMON ISLANDS
SOM	SOMALIA
ZAF	SOUTH AFRICA
KOR	SOUTH KOREA (REP OF KOREA)
ESP	SPAIN
LKA	SRI LANKA
KNA	ST KITTS AND NEVIS
LCA	ST LUCIA
SPM	ST PIERRE AND MIQUELON
VCT	ST VINCENT AND THE GRENADINES
XXA	STATELESS PERSON (ARTICLE 1 OF 1951 CONVENTION)
SDN	SUDAN
SUR	SURINAME
SJM	SVALBARD AND JAN MAYEN ISLANDS
SWZ	SWAZILAND
SWE	SWEDEN
CHE	SWITZERLAND
SYR	SYRIA (ARAB REP)
TWN	TAIWAN (REP OF CHINA)
TJK	TAJIKISTAN
TZA	TANZANIA (UNITED REP OF)
THA	THAILAND
TLS	TIMOR-LESTE
TGO	TOGO
TKL	TOKELAU

CODE	NATIONALITY
TON	TONGA
TTO	TRINIDAD AND TOBAGO
TUN	TUNISIA
TUR	TURKEY
XXT	TURKISH REPUBLIC OF NORTHERN CYPRUS
TKM	TURKMENISTAN
TUV	TUVALU
UGA	UGANDA
UKR	UKRAINE
ARE	UNITED ARAB EMIRATES
UNO	UNITED NATIONS
UNA	UNITED NATIONS AGENCY
UMI	UNITED STATES MINOR OUTLYING ISLANDS
USA	UNITED STATES OF AMERICA
VIR	UNITED STATES VIRGIN ISLANDS
XXX	UNSPECIFIED NATIONALITY
URY	URUGUAY
UZB	UZBEKISTAN
VUT	VANUATU
VEN	VENEZUELA
VNM	VIETNAM
WLF	WALLIS AND FUTUNA ISLANDS
ESH	WESTERN SAHARA
YEM	YEMEN
ZMB	ZAMBIA
ZWE	ZIMBABWE

HSSCCG-10-J-00034 - APPENDIX F

IAFIS IMAGE QUALITY SPECIFICATIONS

1.0 SCOPE AND PURPOSE

These specifications apply to fingerprint scanner systems and printers that will supply fingerprint data to the Integrated Automated Fingerprint Identification System (IAFIS), and to printers and displays within the IAFIS. They provide objective criteria for insuring image quality.

Electronic images must be of sufficient quality to allow for: (l) conclusive fingerprint comparisons (identification or non-identification decision); (2) fingerprint classification; (3) automatic feature detection; and (4) overall Automated Fingerprint Identification System (AFIS) search reliability.

The fingerprint comparison process requires a high fidelity image without any banding, streaking or other visual defects. Finer detail such as pores and incipient ridges are needed since they can play an important role in the comparison. Additionally, the gray-scale dynamic range must be captured with sufficient depth to support image enhancement and restoration algorithms.

The image quality requirements have associated test procedures, which are described in the document Test Procedures for Verifying IAFIS Scanner Image Quality Requirements. These procedures will be used by the Government in acceptance testing to ensure compliance with the requirements, and in performance capability demonstrations as an indication of capability to perform. Equipment shall be tested to meet the requirements in normal operating modes, e.g., scanners shall not be tested at slower than normal operating speeds to meet modulation transfer function specifications. A vendor may recommend alternate testing methods.

2.0 FINGERPRINT SCANNERS

The following subsections describe the image quality performance characteristics required for a fingerprint scanner (live scan and card scan). These specifications require that the scanner shall capture fingerprints at a minimum resolution in both the detector row and detector column directions (also known as 'along-scan' and 'cross-scan' directions) of 500 pixels/inch, plus or minus 5 pixels per inch. The final output delivered image from the scanner system shall have a resolution of 500 pixels/inch, plus or minus 5 pixels per inch, and each pixel shall be gray level quantized to 8 bits. [Requirement

described in the ANSI standard: Data Format for the Interchange of Fingerprint Information, ANSI/NIST-CSL 1-1993.]

CJIS-RS-0010 (V7)

101

January 29, 1999

2.1 Geometric Image Accuracy

The absolute value of the difference "D", between the actual distance "X" between any two points on a target and the distance "Y" between those same two points as measured on the output scanned image of that target, shall meet the following requirements for the value D:

D 0.0007, for 0 X 0.07

D 0.01X, for 0.07 X 1.50

where: D, X, Y are in inches and D = Y - X

The requirement corresponds to a positional accuracy of ± 1% for distances between 0.07 and 1.5 inches, and a constant ± 0.0007 inches (1/3 pixel) for distances less than or equal to 0.07 inches. The geometric image accuracy shall be measured using precision 1 cycle per millimeter Ronchi targets on white Mylar reflective base manufactured by Applied Image, Inc.4

2.2 Modulation Transfer Function

The measured modulation trans fer function (MTF) of the scanner, in both the detector row and detector column directions, and over any region of the scanner's field of view, shall have modulation values which fall within the ranges given in the following MTF table, at the given spatial frequencies:

cyc/mm MTF
1 .905 to 1.00
2 .797 to 1.00
3 .694 to 1.00
4 .598 to 1.00
5 .513 to 1.00
6 .437 to 1.00
8 .312 to 1.00

10 .200 to 1.00

The MTF shall be measured using test chart number M-13-60-1X manufactured by Sine Patterns, Inc.5. The single, representative sine wave modulation in each imaged sine wave frequency pattern is determined from the sample modulation values collected from within that pattern. The sample modulation values are computed from the maximum and minimum levels corresponding to the 'peak' and adjacent 'valley' in each sine wave period. These maximum and minimum levels represent the corresponding locally averaged image gray levels mapped through a calibration curve into target reflectance space, where the local average of gray levels is computed in a direction orthogonal to the sinusoidal variation direction. Sample image modulation is then defined as:

4Applied Image, 1653 East Main Street, Rochester, NY 14526, Phone (716) 482-0300

5Sine Patterns, 236 Henderson Drive, Penfield, NY 14526, Phone (716) 248-5338

CJIS-RS-0010 (V7)

102

January 29, 1999

(maximum - minimum) / (maximum + minimum)

The calibration curve is constructed by performing a least squares linear regression curve fit between the image gray levels of the 14 density patches in the test target and the corresponding target reflectance values. The scanner MTF at each frequency is then defined as:

MTF = representative image modulation / target modulation

[Target modulations and target density patch values are supplied with the test target by the manufacturer.]

2.3 Signal-to-Noise Ratio

Both the ratio of signal to white noise standard deviation and the ratio of signal to black noise standard deviation of the digital scanner shall be greater than or equal to 125 using the following procedure:

1) A random 0.25 inch x 0.25 inch test field within the image area is chosen and the white reference target, Munsell6 N9-white matte, is placed in the test field.

2) A white test population of 8-bit reflectance values from at least 1000 samples within the test field are collected. The average value and standard deviation are computed from this test population.

3) Steps 1 and 2 are repeated for the black reference target, Munsell N3 - black matte.

4) The signal to noise ratio (SNR) is computed as the difference between average white and average black values, alternately divided by the white noise standard deviation ('white SNR') and the black noise standard deviation ('black SNR').

Note: The scanner shall be set up such that the white reference target is below scanner saturation level, and the black reference target is above scanner dark current level. Also, care should be taken, via direct visual or visual display observation, to avoid areas of dust, pinholes, scratches, or other imperfections on the target when selecting the sub-area for the 1000 samples.

6 Munsell-Macbeth, P.O. Box 230, Newburgh, NY 12551, Phone (914) 565-7660

2.4 Gray-Scale Range of Image Data

At least 80% of the captured individual fingerprint images shall have a gray-scale dynamic range of at least 200 gray levels and at least 99% shall have a dynamic range of at least 128 gray levels. For this requirements section, 'dynamic range' is defined as the total number of gray levels that have signal content from the fingerprint image. Fingerprint card format lines, boxes, and text shall be excluded from the dynamic range computation and white surround in the immediate vicinity of a given fingerprint shall be

included in the dynamic range computation (dashed box at right). Compliance with these dynamic range requirements shall be verified using a stratified sample of fingerprint cards assembled by the Government.

The intent is to avoid excessively low contrast images. Live-scan systems and card scanners at a booking station can control dynamic range by rolling the prints properly. However, with central site or file conversion systems, where a variety of card types and image qualities are encountered, adaptive processing may be necessary. The 8-bit quantization of the gray-scale values for very low contrast fingerprints needs to more optimally represent the reduced gray-scale range of such fingerprints. In the example histogram accompanying this section, the gray-scale values divide up the range from A to B. The parameters A and B are stored with the image to provide an audit trail.

2.5 Gray-scale Linearity

Using the 14 gray patches in the Sine Patterns, Inc. test target M-13-60-1X as the scanner input (independent variable), with their manufacture-supplied reflectance values, none of the corresponding 14 scanner output gray levels (dependent variable) shall deviate by more than 7.65 gray levels from a linear, least squares regression line fitted between the two variables. The output sample values within an area of at least 0.25 x 0.25 inches shall be utilized to compute the average output gray level for each patch.

2.6 Output Gray Level Uniformity

Output gray level uniformity shall be determined by scanning both a white reference target, Munsell N9 - white matte, and a black reference target, Munsell N3 - black matte. The scanner shall be set up such that the white reference target is below scanner saturation level, and the black reference target is above scanner dark current level in the respective tests. Using the white target as the scanner input, the following three requirements shall be met:

---

(1) The outputs of any two adjacent rows or columns of length 9 pixels or greater shall not have mean gray levels that differ by more than 2.5 gray levels.

(2) For all pixels within a 0.25 inch x 0.25 inch area ('quarter inch area') located in any region of the total scanner field of view, no individual pixel's gray level shall vary from the mean gray level by more than 22.0 gray levels.

(3) For any two non-contiguous quarter inch areas located anywhere in the total scanner field of view, the mean gray levels of the two quarter inch areas shall not differ by more than 12.0 gray levels.

And, using the black target as the scanner input, the following three requirements shall be met:

(1) The outputs of any two adjacent rows or columns of length 9 pixels or greater shall not have mean gray levels that differ by more than 1.0 gray levels.

(2) For all pixels within a 0.25 inch x 0.25 inch area ('quarter inch area') located in any region of the total scanner field of view, no individual pixel's gray level shall vary from the mean gray level by more than 8.0 gray levels.

(3) For any two non-contiguous quarter inch areas located anywhere in the total scanner field of view, the mean gray levels of the two quarter inch areas shall not differ by more than 3.0 gray levels.

3.0 LATENT PRINT SCANNERS

The following subsections describe the image quality performance characteristics required for a latent print scanner operating in a 1000 pixels/inch mode. These specifications require that the scanner shall capture fingerprints at a minimum resolution in both the detector row and detector column directions (also known as 'along-scan' and 'cross-scan' directions) of 1000 pixels/inch. The final output delivered image from the scanner system (at the 1000 ppi setting) shall have a resolution of 1000 pixels/inch, plus or minus 10 pixels per inch, and each pixel shall be gray level quantized to a minimum of

8 bits. The complete latent print specification consists of all requirements given in this Section, plus all non-conflicting requirements given in Section 2.0 Fingerprint Scanners.

3.1 Geometric Image Accuracy

The absolute value of the difference "D", between the actual distance "X" between any two points on a target and the distance "Y" between those same two points as measured on the output scanned image of that target, shall meet the following requirements for the value D:

D 0.0005, for 0 X 0.07

D 0.0071X, for 0.07 X 1.50

where: D, X, Y are in inches and D = Y - X

The requirement corresponds to a positional accuracy of ± .71% for distances between 0.07 and 1.5 inches, and a constant ± 0.0005 inches (½ pixel) for distances less than or equal to 0.07 inches. The geometric image accuracy shall be measured using precision 1 cycle per millimeter Ronchi targets on white Mylar reflective base manufactured by Applied Image, Inc.7

3.2 Modulation Transfer Function

The measured modulation transfer function (MTF) of the scanner, in both the detector row and detector column directions, and over any region of the scanner's field of view, shall have modulation values which fall within the ranges given in the following MTF table, at the given spatial frequencies:

cyc/mm	MTF
1	0.925 to 1.00
2	0.856 to 1.00
3	0.791 to 1.00
4	0.732 to 1.00
5	0.677 to 1.00
6	0.626 to 1.00
8	0.536 to 1.00

7Applied Image, 1653 East Main Street, Rochester, NY 14526, Phone (716) 482-0300

cyc/mm MTF
10 0.458 to 1.00
12 0.392 to 1.00
14 0.336 to 1.00
16 0.287 to 1.00
18 0.246 to 1.00
20 0.210 to 1.00

The MTF shall be measured using test chart number M-13-60-1X manufactured by Sine Patterns, Inc.8. The single, representative sine wave modulation in each imaged sine wave frequency pattern is determined from the sample modulation values collected from within that pattern. The sample modulation values are computed from the maximum and minimum levels corresponding to the 'peak' and adjacent 'valley' in each sine wave period. These maximum and minimum levels represent the corresponding locally averaged image gray levels mapped through a calibration curve into target reflectance space, where the local average of gray levels is computed in a direction orthogonal to the sinusoidal variation direction. Sample image modulation is then defined as:

(maximum - minimum) / (maximum + minimum)

The calibration curve is constructed by performing a least squares linear regression curve fit between the image gray levels of the 14 density patches in the test target and the corresponding target reflectance values. The scanner MTF at each frequency is then defined as:

MTF = representative image modulation / target modulation

[Target modulations and target density patch values are supplied with the test target by the manufacturer.]

8Sine Patterns, 236 Henderson Drive, Penfield, NY 14526, Phone (716) 248-5338

CJIS-RS-0010 (V7)

107

January 29, 1999

4.0 IAFIS DISPLAY SPECIFICATIONS

Two types of displays are required. One is for the ten-print examiner and document processing. The other is for the latent examiner.

4.1 Ten-print / Document Processing Display

The ten-print/document processing display shall meet the following performance levels:

Parameter Value Comments
Colors 256 8 bits/pixel
Number ofaddressable pixels 1280 x 1024
Pixel size 0.28 mm (max) width at 50% amplitudeat center of display
Active display area 14" x 10.5" (min) Landscape mode
Display refresh at least 72 Hznoninterlaced Minimizes flickerrate
Video bandwidth at least100 MHz
Luminance 33 fL (min) of white area
Video pulse rise & fall time 3 nanosec. (max) ensures no visible smearing
Geometric pixel location error ±1.5% (max) No point varies more then 1.5%from its correct position
Operator controls brightness, contrast on front panel
Brightness Uniformity ±15% of meandeviation (max) over entire display at low, medium and high brightness

---

4.2 Latent Print Comparison Display

The other display is for use by the FBI's latent fingerprint examiners. Because this display will be used to support latent fingerprint comparisons, the resolution and brightness (luminance) requirements are higher. The display shall be a monochrome cathode ray tube display, which shall meet the following performance levels:

Parameter Value Comments
Gray levels 8 bits/pixel @CRT video input
Number of addressable pixels 1600 x 1200
Pixel size 0.19 mm (max) width at 50% amplitude at center of display
Active display area 14" x 10.5" (min) Landscape mode
Display refresh rate at least 72 Hz noninterlaced Minimizes flicker
Video bandwidth at least 100 MHz
Luminance 50 fL (min) of white area

Video pulse rise & fall time 3 nanosec. (max) ensures no visible smearing
Geometric pixel location error ±1.5% (max) No point varies more then 1.5% from its correct position
Operator controls brightness, contrast on front panel
Brightness Uniformity ±15% of mean deviation (max) over entire display at low, medium and high brightness

The ambient lighting in the work area is expected to be a combination of natural and fluorescent lighting.

CJIS-RS-0010 (V7)

109

January 29, 1999

5.0 PRINTER SPECIFICATIONS

The fingerprint examiners in the IAFIS environment will depend upon softcopy images to make comparisons and will require hardcopy images in certain instances. Some contributors will print cards from live scan or card scan devices for submission to the FBI. In all such cases the images will be mapped from their digital form to high resolution printing devices. The printed images must be of sufficient quality to support all phases of identification, including conclusive fingerprint comparisons (identification or non-identification decision).

Two classes of printing devices are required. The first is intended to support fingerprint card reproduction. These printers will be used within the IAFIS environment and by submitters who choose to print and mail their live scan results. The printers should provide high throughput, low-cost-per-copy, non-fading output. This monochrome printer shall perform at the following minimum levels:

Gray levels 16

Paper size 8" x 8" (min)

Resolution 500 dots/inch (min.), where each pixel is capable of producing 16 gray levels

A second class of printer is required to support the investigative fingerprint comparison function. Continuous tone monochrome output is required. This printer shall perform at the following minimum levels:

Gray levels 8-bit continuous-tone gray-scale

Paper Production of output paper print shall not require liquid processing

Paper size 8" x 11"

Resolution At least 500 pixels per inch, where each pixel is capable of producing 256 gray levels from an 8 bits/pixel input

CJIS-RS-0010 (V7)

110

January 29, 1999
